



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/381,056	12/21/1999	PAUL MERTES	2345/86	3457

26646 7590 03/09/2004

KENYON & KENYON
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER

FIELDS, COURTNEY D

ART UNIT	PAPER NUMBER
----------	--------------

2137

16

DATE MAILED: 03/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

1/2

Office Action Summary

Application No.

09/381,056

Applicant(s)

MERTES ET AL.

Examiner

Courtney D. Fields

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 December 2003.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 4-7 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 4-7 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 15 December 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

Response to Arguments

1. Applicant's arguments filed 15 December 2003 have been fully considered but they are not persuasive.
2. Referring to the rejection of claim 4, the Applicant contends that the prior art (Fischer) does not teach nor disclose the features of producing at least one encryption key pair including a public part and a secret part, marking the public part of the encryption pair, after marking the public part of the pair, transmitting the encryption key pair to the trust center, unequivocally assigning the one of the encryption pair to a user, causing the trust center to check the assignment of the encryption key pair by using a public part of the signature key pair, after the check is successful, the trust center produces a new certificate by using one of the public part of the previously generated key pair and the public part of the encryption key pair, encrypting a new certificate using the public part of the encryption key pair. The Examiner disagrees and asserts that Fischer does teach the elements of claim 4, in Column 6, lines 14-16, each user is issued (assigned) a public encrypting key and an associated private secret decrypting key. A digital signature is accompanied by at least one valid certificate which specifies the identity of the signer and the authorization which the signer has been granted in Column 7, lines 21-29. The trust center (Bureau of Standards) participates in a public key cryptosystem in which participants are registered in the system and assigned public keys which they are authorized to use with the meta-certifier in Column 8, lines 4-16. After each of the required signatures has been created, the certificate's signatures and the respective certificates are used for generating new certificates (subcertifying

terminal user A). In this manner, the signed message unequivocally contains the hierarchy of certificates and the assigned signatures which verifies that terminal A user's identity and his authority. Therefore, when terminal B user creates a new authorizing certificate for terminal A user, the certificate will include a specification of terminal A's identity with terminal A's public key encryption key. (See Column 8, lines 50-67, Column 9, lines 1-11)

3. In addition, claim 7 which contains analogous features to claim 4, is rejected for the same reasons as for claim 4. Therefore the rejection of claims 4-7 are maintained in view of the reasons above and in view of the reasons below.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 4-~~8~~⁷ are rejected under 35 U.S.C. 102(b) as being anticipated by Fischer U.S. Patent No. 4,868,877. Referring to claim 4, Fischer discloses a trusted authority (Bureau of Standards or the country's largest bank) that participates in a public key cryptosystem with the users of General Motors. Users are given meta-certified keys with three different levels, once the highest level is obtained, a certificated is made to meet the limitations of each user in Column 8, lines 4-49. Each of the users has a public

encryption key and an associated private secret key pair in Column 6, lines 14-16. By using a portion of the privately held signature key, a message can be signed with digital signature if the public key is used to encrypt the result of the hash, compare it with the recomputed hash of the private key and confirm the signed message in Column 7, lines 5-20. In accordance to a digital signature, a valid certificate must be granted. Therefore, Fischer reveals once user A's public/private key pair is obtained by user B, the public key insures certification and allows user B to create a new certificate. User B uses it's secret private key and decrypts the encrypted signature of the new certificate which becomes part of user A's new certificate packet, in Column 13, lines 57-68, Column 14, lines 1-7.

Referring to claim 5, Fischer discloses the claimed limitation of having an additional key pair in Figure 4. Fischer enables user A signature to be co-signed by user C's public and secret private key in Column 13, lines 9-11. The public key as shown in Figure 4, is incorporated inside a certificate that is used to perform the signature for user A in Column 13, lines 15-21.

Referring to claim 6, Fischer discloses the claimed limitation of the highest trust level 3, which is for a meta certifier whose public key and certificates are established and known without the assistance of another user, and also the certifier takes responsibility only for identifying (checking the correctness) the entities whose public keys it certifies in Column 9, lines 50-54. Fischer shows the steps of utilizing a public encryption key transmitted with a certificate and verifying the signature is performed in Figure 3 and

Column 11, lines 54-62. After the verification is done, Fischer shows a check and validation for each new certificate is performed in Column 17, lines 47-63.

Conclusion

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 703-305-8293. The examiner can normally be reached on Mon - Thu 7:00 - 5:00 pm; off every Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 703-308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 872-9306 for regular communications and (703) 872-9306 for After Final communications.

Application/Control Number: 09/381,056
Art Unit: 2137

Page 6

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.



cdf
March 5, 2004



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100